

(01/26/1998)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION UU 15 1999

Precedence: PRIORITY

Date: 10/06/1999

To: All Field Offices

Attn: ADIC;

WCM/HLL National Security

SAC

Attn: SSA [REDACTED]

NIPC/CIOS/CIU (Room 11719)

From: Newark

FTRA-2

Contact: [REDACTED]

Approved By: [REDACTED] *[Signature]*

Drafted By: [REDACTED] *[Signature]*

Case ID #: 288A-NK-99660 (Pending)
288A-HQ-1281779 (Pending) *-38*

Title: [REDACTED]
UNSUB(S), AKA VICODINES;
ET AL;
MELISSA VIRUS;
IMPAIRMENT - INFO SYSTEMS;

b6
b7C

Synopsis: To request all field offices to gather and report damages to victims infected by the Melissa Macro Virus.

Details: For information of receiving offices, the Newark Division is requesting the assistance of all field offices in identifying and reporting damages caused by the Melissa Macro Virus ("MMV") to corporations, organizations and agencies, including federal, state and local government, in their respective territories. The following is a summary of investigative activities and developments pertaining to the ongoing investigation of the MMV:

On 3/26/99, the MMV was proliferated on an America Online ("AOL") network news server through a posting to the alt.sex newsgroup using a stolen AOL account belonging to the screen name [REDACTED]. An attachment to the posting contained names of alleged "cracked" pornographic websites. The newsgroup posting contained a file called list.zip which contained a document called list.doc. The list.doc document contained the MMV. The MMV infected those using Microsoft Windows, and Microsoft Word, Outlook and Outlook Express. MMV was coded to send an infected document to the first (50) addresses in each users email address book. The compounding effect of MMV proliferation caused many email servers throughout the U.S. and

b6
b7C

SA C/SF 288A-AI-68562-106
10/06/99 [REDACTED] *[Signature]*
Lead to [REDACTED] *[Signature]*
288A-NA-99

b6
b7C

To: All Field Offices From: Newark
Re: 288A-NK-99660, 10/06/1999

rest of the world to crash. Systems administrators and Information Technology personnel scrambled to mitigate the effects of MMV on their systems.

On 4/1/99, the Newark Division and the New Jersey State Police (NJSP) High Technology Crime Unit arrested [REDACTED] pursuant to a state of New Jersey arrest warrant obtained from Monmouth County Superior Court Judge [REDACTED]. [REDACTED] was charged with second degree offenses of interruption of public communication, conspiracy to commit the offense and attempt to commit the offense, third degree theft of computer service, and third degree damage or wrongful access to computer systems relating to the propagation of the computer macro virus known as "MELISSA". Earlier that evening, prior to the arrest of [REDACTED] the Newark Division and the NJSP executed a state of New Jersey search warrant at [REDACTED] residence [REDACTED].

b6
b7C

The initial information leading to the arrest and execution of search warrants came from America Online, Inc., Dulles, VA, [REDACTED] contacted the State of New Jersey Attorney General's Office with lead information with respect to MELISSA. The State Attorney General's Office enlisted the NJSP High Technology Crime Unit who in turn enlisted the assistance of the Newark FBI NIPC squad.

Additionally, Newark and the NJSP have executed search warrants at [REDACTED]

[REDACTED] On 4/16/99, Newark and the NJSP seized from AT&T (14) back-up cartridges and other computer evidence from [REDACTED]

b6
b7C

The District of New Jersey U.S. Attorney's Office and the Attorney General's Office for the state of New Jersey anticipate returning simultaneous indictments on or about October 31, 1999. To aid the prosecution, it has been requested that Newark obtain detailed victim information relating to damages caused by the Melissa Macro Virus. This information is critical to the prosecution of captioned subject(s).

Questions regarding this communication should be directed to SA [REDACTED] Newark Division's NIPC Squad at Franklin Township RA, telephone [REDACTED]

b6
b7C

To: All Field Offices From: Newark
Re: 288A-NK-99660, 10/06/1999

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

Newark requests all field offices to identify victim corporations, organizations and agencies, including federal, state and local government, in their respective territories infected by the Melissa Macro Virus ("MMV"). Newark recognizes that this is an inherently difficult task and asks field offices to utilize liaison contacts, including those developed through the Key Asset and InfraGard Programs where applicable. Field divisions are also asked to identify and follow-up on any complaints previously received relating to MMV and report those instances to Newark. If necessary, Federal Grand Jury subpoenas will be made available when requested.

Victims should report, in dollars, their best calculation of the damages caused by MMV. Victims may be asked to verify their reported damages in federal court. Information requested should detail the nature and extent of damages caused by MMV including, but not limited to, the following areas: email servers, desktop computers and other computer hardware affected; computer system downtime; personnel time, including overtime, for corrective action; lost productivity; lost contracts and missed business opportunities; diminished profits; consulting expenses; infrastructure costs; lost customers; and sensitive data leakage.

Set Lead 2:

NATIONAL SECURITY

AT WASHINGTON, DC

NIPC/CIOS/CIU - Read and clear.

♦♦